Orin Snyder (*pro hac vice*)
osnyder@gibsondunn.com
GIBSON, DUNN & CRUTCHER LLP
200 Park Avenue
New York, NY 10166-0193
Telephone: 212.351.4000
Facsimile: 212.351.4035

Joshua S. Lipshutz (SBN 242557)
jlipshutz@gibsondunn.com
GIBSON, DUNN & CRUTCHER LLP
1050 Connecticut Avenue, N.W.
Washington, DC 20036-5306
Telephone: 202.955.8500
Facsimile: 202.467.0539

Kristin A. Linsley (SBN 154148)
klinsley@gibsondunn.com
Brian M. Lutz (SBN 255976)
blutz@gibsondunn.com
GIBSON, DUNN & CRUTCHER LLP
555 Mission Street, Suite 3000
San Francisco, CA 94105-0921
Telephone: 415.393.8200
Facsimile: 415.393.8306

Attorneys for Defendant Facebook, Inc.

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

IN RE: FACEBOOK, INC. CONSUMER PRIVACY USER PROFILE LITIGATION,

This document relates to:

ALL ACTIONS

CASE NO. 3:18-MD-02843-VC

REPLY IN SUPPORT OF MOTION OF DEFENDANT FACEBOOK, INC. TO DISMISS PLAINTIFFS' FIRST AMENDED CONSOLIDATED COMPLAINT

Judge: Hon. Vince Chhabria
Courtroom 4, 17th Floor
Hearing Date: May 29, 2019
Hearing Time: 10:30 a.m.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes & Rules

Other Authorities

I. INTRODUCTION

This multi-district litigation was established to consolidate dozens of cases arising out of the Cambridge Analytica news coverage of March 2018. After more than a year of litigation, Plaintiffs seem to have concluded that they have no viable claims against Facebook arising out of those events. Instead, switching gears, they attempt to re-cast the case by incanting buzzwords and asserting half-baked allegations gleaned from other news articles—"device manufacturers," "business partners," "Whitelisted apps," "metadata." In their opposition brief, Plaintiffs try to jumble all of these concepts together, invoke generic concerns about the privacy of their online data, assert broadly that Facebook is a bad actor, and hope one of their 49 claims will stick. But while Plaintiffs' generalized privacy concerns may be appropriate subjects before regulators and legislatures, they give rise to no actionable legal claims.

Plaintiffs ask this Court to create brand-new privacy interests that no federal court has ever before recognized—not at common law, not under any state or federal statute, not under the Supreme Court's decision in *Spokeo*, and not under the Ninth Circuit's decision in *Eichenberger*. In Plaintiffs' words, the "[d]isclosure of private information is itself the injury." Pls.' Opp. to Mot. to Dismiss 6 (Apr. 12, 2019) ("Opp."), Dkt. 266. Plaintiffs do not cite a single case even remotely supporting this boundless definition, much less suggesting that the disclosures or data-sharing at issue here would give rise to Article III standing. If adopted, Plaintiffs' arguments would transform privacy law in this country, opening the courthouse door to any plaintiff who alleges that their online data was shared with anyone for any reason—a commonplace feature of the Internet that occurs countless times every day. That is not, and cannot be, the law. This case should be dismissed.

II. SORTING OUT PLAINTIFFS' THEORIES

Before addressing Plaintiffs' legal arguments, it is important to untangle the stray issues that Plaintiffs are mushing together in an attempt to survive dismissal, and to explain why none supports continued litigation.

1. Kogan & Cambridge Analytica. The bulk of the Plaintiff-specific allegations in the complaint relate to data sharing with Kogan's app (thisisyourdigitallife) and Kogan's unauthorized sale of user data to Cambridge Analytica. But, as Facebook has set forth in several rounds of briefing, Plaintiffs' Cambridge Analytica allegations fail for numerous reasons.

No sensitive information. Plaintiffs still have not explained how the sharing of their data with Cambridge Analytica caused them to suffer any real-world, Article III injury. Kogan's app did not obtain financial information, social security numbers, or any other information that placed Plaintiffs at any risk of identity theft or any other economic injury. The data Plaintiffs' friends shared with Kogan also was, by definition, information that Plaintiffs had already shared with others on Facebook, and was not the type of highly sensitive information that has traditionally given rise to a privacy injury. Plaintiffs have even abandoned their speculative allegation that they were among the 1,500 users whose Facebook messages were acquired by Kogan. *See* Opp. 5-6 (no argument that Facebook obtained Plaintiffs' messages). The only consequence of Cambridge Analytica's acquisition of user data was that some users may have received targeted advertisements, which is not an actionable Article III injury.

Consent. As Plaintiffs have previously acknowledged, Plaintiffs consented to sharing their data with Kogan's app. Mem. of Law in Support of Facebook, Inc.'s Mot. to Dismiss 20 (Mar. 15, 2019) ("MTD"), Dkt. 261-1. As Plaintiffs once admitted, Kogan only acquired Facebook users' data consistent with the users' privacy settings. Prior Compl. ¶¶ 121-22. Plaintiffs argue that they did not consent to *Kogan* sharing that data with *Cambridge Analytica*. Opp. 14. But no one disputes that point. Facebook never promised users that it was impossible for third-party apps to misuse data. Facebook truthfully informed users that apps acquiring their data via friend permissions "will only be *allowed* to use that content and information in connection with that friend," First Am. Consolidated Compl. ¶ 597 (Feb. 22, 2019) ("Compl.") (quotation marks omitted), Dkt. 257, but expressly warned users that "games, applications and websites are created and maintained by other businesses and developers who are not part of, or controlled by, Facebook," D.D., Ex. 45 at 8 (Dec. 11, 2012 Data Use Policy).

2. Other third-party apps. Plaintiffs also complain about "tens of thousands" of other third-party apps (Opp. 8)—but they do not claim to have actually used, or have friends that used, *any* of those apps. Plaintiffs allege it is "virtually certain" other apps obtained their data, *id*., but that type of argument is exactly the type of standing argument the Supreme Court rejected in *Clapper v. Amnesty International, USA*, where the plaintiffs could "merely speculate and make assumptions about whether their communications" had been acquired by the government. 568 U.S. 398, 411 (2013); *see also id.* at 410 (rejecting the "objectively reasonable likelihood" standard for standing).

In any event, Plaintiffs consented to the sharing of data with third-party apps, just as they consented to sharing data with Kogan's app. Facebook explained to users how they could limit sharing with apps via their app settings—both in the Data Use Policy and SRR. MTD 28. Plaintiffs argue that Facebook misled users when it explained in the SRR that "you can control how [content and information you post on Facebook] is shared through your privacy [hyperlinked] ***and*** application [hyperlinked] settings" because, in their view, the word "and" suggested that privacy settings alone were sufficient to limit apps' access to user data. Opp. 12, 36 (emphasis added) (quotation marks omitted). But that is not how English works: the word "and" indicates that *both* items in a two-item list are necessary, whereas "or" connotes that either item is sufficient. *See* Bryan A. Garner, Garner's Modern English Usage 50 (4th ed. 2016) (entry for "and/or"). In other words, the SRR told users that they should consult ***both*** their privacy ***and*** app settings in determining how to "control" the sharing of their content. Privacy settings govern "who sees user information *on Facebook*," Opp. 13 (emphasis added) (quotation marks omitted), whereas application settings govern data sharing with apps, but the two are interconnected—as Facebook clearly explained in its Data Use Policy: "if you share something on Facebook, ***anyone who can see it can share it with others,*** including the games, applications, and websites they use." D.D., Ex. 45 at 9 (emphasis added).

3. "Whitelisted" Apps. Plaintiffs try to state a claim regarding so-called "Whitelisted" apps. But Whitelisted apps are just a species of third-party apps that had custom agreements with Facebook. From a user's perspective, that distinction is immaterial; Facebook never promised users that apps would access data *only* using an off-the-rack API. For all third-party apps (including "White-listed" apps), users' consent was required before their data was shared. *See* Prior Compl. ¶¶ 121-22.

Plaintiffs lack standing with respect to Whitelisted apps because they have not alleged that *any* of the Whitelisted apps acquired *their* data. Plaintiffs ask to be relieved of this basic pleading requirement because "Plaintiffs do not know what Apps … are used by their Friends" and "Facebook has largely hidden" the names of these apps. Opp. 7-8. Not so. Plaintiffs' own complaint identifies several apps they believe to have been among those "Whitelisted," *e.g.*, Compl. ¶¶ 497, 502, 505-06, 508, 510, yet Plaintiffs say they have no idea whether their friends used any of these apps—not even on information and belief. Plaintiffs' lack of knowledge with respect to their friends' use of Whitelisted apps shows

either that they have not conducted the necessary pre-filing investigation on this issue, *see* Fed. R. Civ. P. 11(b), or that their investigatory findings did not help their cause. This is a classic pleading failure.

4. Device Manufacturers. Plaintiffs' allegations regarding device manufacturers (who Plaintiffs sometimes mislabel "Business Partners") are similarly not actionable. As with the Whitelisted apps, Plaintiffs do not allege which device manufacturers (if any) actually obtained their information.[1] Plaintiffs allege that "Apple, Samsung, AT&T, Sprint, T-Mobile, and Verizon" are among the device manufacturers at issue, Opp. 7, but Plaintiffs apparently have not inquired whether any of their friends used these devices.

Regardless, Plaintiffs consented to Facebook's partnerships with device manufacturers. The Data Use Policy explained that Facebook would provide data to "companies that help us provide … the services we offer" including those who "help host our website." Compl. ¶ 616 (quotation marks omitted). And the device manufacturers here did exactly that—they "buil[t] Facebook's Platform on different devices and operating systems." *Id.* ¶ 486. In other words, when users sought to engage with Facebook on certain devices, those devices unsurprisingly needed data from Facebook to perform that function. That is not injury in any sense of the word, and Plaintiffs do not (and cannot) allege that the device manufacturers did anything improper with the data they accessed. Plaintiffs assert that these companies "received far more data than what was necessary" to support Facebook's website, Opp. 16, but the examples they cite relate to entities that Plaintiffs have not identified as being among Facebook's "Business Partners" (e.g., Compl. ¶ 557, referencing the New York Times) or quote from sources indicating that the company in question obtained only publicly available information. *See id.* ¶ 559 (citing Gabriel J.X. Dance, et al., *As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants*, N.Y. Times (Dec. 18, 2018) (reporting that Microsoft Bing accessed only "public data")).

5. Advertisers. Plaintiffs no longer allege that targeted advertising *simpliciter* (which Plaintiffs term "psychographic profiling") is a privacy injury sufficient to satisfy Article III's injury-in-fact require-

[1] Only two plaintiffs allege the type of smartphone they used to access Facebook (an iPhone), but those two plaintiffs do not allege they shared on Facebook the type of data that Apple allegedly obtained. Compl. ¶¶ 226-233, 256-263, 563.

ment. *See* Opp. 5-8 (no reference to advertising). That abandonment is understandable; Plaintiffs previously admitted there is "nothing wrong" with targeted advertising, Prior Compl. ¶ 110, and they consented to receive targeted advertisements via the Data Use Policy, which explained that Facebook "allow[s] advertisers to target a category of a user … by bundling characteristics that we believe are related to the category." D.D., Ex. 45 at 11-12. Equating these "characteristics" with "psychographic profiles" is nothing but wordplay, and does not negate Plaintiffs' lawful consent.

Instead, Plaintiffs now allege that Facebook "sold" or otherwise gave data to third parties to use for advertising purposes. Opp. 15. But Plaintiffs have no support for that false allegation. To be clear, Facebook does not sell user data, period, as Plaintiffs surely are aware. *See* Fed. R. Civ. P. 11(b). Nor does Facebook provide user-identifiable data to advertisers. All information shared with advertisers first has "removed from it anything that personally identifies you." D.D., Ex. 45 at 11. Plaintiffs say that some advertisers obtained data because the same companies are third-party app developers or device manufacturers. But in those circumstances, users were sharing data with those companies consensually for non-advertising purposes, subject to the limitations described above—it does not mean Facebook provided data to those companies for advertising purposes. It simply reflects the reality that companies can wear different hats in different circumstances.

6. Photograph Metadata. Plaintiffs allege that Facebook "'stripped' privacy metadata from photos and videos" when it transmitted data to third parties, Opp. 13-14, but the relevance of that allegation is unclear. A user's Facebook privacy settings with respect to a particular photo or video—for example, whether it can be shared with the user's "Friends" or "Friends of Friends"—is different from the policies governing data shared by Facebook users with third-party apps. D.D., Ex. 42 at 6. Specifically, the app must comply with Facebook's Platform Policy, which requires the app to use the data only in connection with enhancing the user's on-app experience, Compl. ¶ 597; D.D., Ex. 23 at 5-6, and with the app's own agreement with users. Compl. ¶ 612.

7. The 2012 FTC Consent Order. Plaintiffs argue that the FTC's 2012 Consent Order "allayed" their concerns regarding data sharing with third-party apps, Opp. 43, because, according to Plaintiffs, the Consent Order requires Facebook "*not* to share user data with third-party Apps and websites unless Facebook had 'clearly and prominently disclose[d] to the user, separate and apart from' the SRR and the

Data Policy," that the information would be disclosed. Opp. 20-21. But that allegation is implausible because the 2012 Consent Order expressly contradicts that assertion. The requirement that Plaintiffs reference applies *only* if the sharing "materially exceeds the restrictions imposed by a user's privacy setting(s)," a term that includes app settings. Consent Order at 4, https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf; *id.* at 3 (defining "[p]rivacy setting" to "include any control or setting provided by [Facebook] that allows a user to restrict which individuals or entities can access or view covered information"). And Plaintiffs' own admissions make clear that the sharing of data with third-party apps, including friend re-sharing, was done only when *consistent* with users' privacy settings. Prior Compl. ¶¶ 121-22. In fact, the Consent Order expressly *allows* Facebook to continue friend re-sharing of user data with third-party apps *without* additional disclosures: As stated in the second paragraph of Part II, "[n]othing in Part II will … require [Facebook] to obtain affirmative express consent for sharing of a user's nonpublic user information initiated by another user authorized to access such information, provided that such sharing does not materially exceed the restrictions imposed by a user's privacy setting(s)." Consent Order at 4, *supra*. Thus, any user concerned about friends re-sharing their data would have known, after reading the FTC's widely publicized 2011 Complaint and 2012 Consent Order, that the practice was ongoing and consistent with Facebook's disclosures.

III. LEGAL ARGUMENTS

Turning now to Plaintiffs' legal arguments, it is clear that their claims cannot survive dismissal. Plaintiffs' claims continue to suffer the same flaws that have plagued them from day one: lack of standing, consent, and an inability to make the facts fit the elements of any cause of action.

A. Plaintiffs Lack Standing

As an initial matter, the injuries Plaintiffs assert are insufficient to establish Article III standing.

1. Plaintiffs allege no cognizable invasion of privacy

Despite repeated attempts over the past year, Plaintiffs still cannot articulate a concrete, real-world, "*de facto*" privacy injury that satisfies the Article III standing requirement. *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1548 (2016). To the contrary, the privacy injuries they assert would invent a brand-new privacy right and stretch the injury-in-fact requirement beyond recognition. We address each in turn.

Plaintiffs consented to the sharing of their Facebook data. Plaintiffs lack standing because they consented to the disclosure of their information, depleting any reasonable expectation of privacy. *See* MTD 8-19; *Warth v. Seldin*, 422 U.S. 490, 500 (1975) (standing "turns on the nature and source of the claim asserted"). Asking whether Plaintiffs consented to the disclosure does not "conflat[e] the standing inquiry with . . . merits questions." Opp. 6. There can be no privacy interest or reasonable expectation of privacy unless information is private in the first place, and that requires considering whether Plaintiffs consented to disclosing the information. Plaintiffs ask this Court to "assume that Facebook will not be able to establish" that Plaintiffs consented to the complained-of practices, *id.* 11, but jurisdiction is not founded on assumptions. Rather, a "Rule 12(b)(1) jurisdictional attack" such as this one, where Facebook "asserts that the allegations contained in a complaint are insufficient on their face to invoke federal jurisdiction," requires a court to "resolve[]" the challenge "as it would a motion to dismiss under Rule 12(b)(6): . . . determin[ing] whether the allegations are sufficient as a legal matter to invoke the court's jurisdiction." *Phillips v. Apple Inc.*, 2016 WL 1579693, at *3 (N.D. Cal. Apr. 19, 2016) (quoting *Safe Air for Everyone v. Meyer*, 373 F.3d 1035, 1039 (9th Cir. 2004), and *Leite v. Crane Co.*, 749 F.3d 1117, 1121 (9th Cir. 2014)). If Plaintiffs consented to the complained-of practices—which they did—then Plaintiffs had no expectation of privacy, and thus lack standing. *Larroque v. First Advantage LNS Screening Sols., Inc.*, 2016 WL 4577257, at *5 (N.D. Cal. Sept. 2, 2016) (dismissing for lack of standing and rejecting invasion-of-privacy injury because plaintiff "agreed to the release of her private information, *eliminating any argument that her privacy was somehow invaded*" (emphasis added)).

The sharing of data alone is not a concrete injury. Even if there had been no consent, the *type* of information Plaintiffs claim was shared—photos and videos that users posted to Facebook, religious and political beliefs, relationship posts, and "the pages they had liked," Compl. ¶ 748—is not the type of information that has historically given rise to a privacy injury when shared. Plaintiffs seem to concede this point in their opposition brief. *See, e.g.*, Opp. 6 n.8 (conceding that "misappropriation of location data" has been held insufficient to constitute standing, as have "zip codes" and "names and driver's license numbers"). Plaintiffs contend that "[i]nvasion of a privacy interest confers standing under Article III, even without further harm." *Id.* 5. But two pages later, they concede the contrary,

agreeing with Facebook that "[n]ot every data breach discloses information *sufficiently sensitive* to constitute an invasion of a legally protected privacy interest." *Id.* 7 (emphasis added). As many courts have held, "the claimed loss of" "personal identifying information"—such as names, addresses, billing information, or even credit card numbers—"does not constitute a concrete harm sufficient for standing purposes." *Dugas v. Starwood Hotels & Resorts Worldwide, Inc.*, 2016 WL 6523428, at *6 (S.D. Cal. Nov. 3, 2016).[2] Article III does not confer standing "based on nothing more than the unauthorized disclosure of personal information." *In re Google, Inc. Privacy Policy Litig.*, 2012 WL 6738343, at *5 (N.D. Cal. Dec. 28, 2012). And here, Plaintiffs cannot allege even that much because they authorized the disclosures at issue.

Plaintiffs have no case law supporting their argument. Plaintiffs rely primarily on the Ninth Circuit's decision in *Eichenberger* to support their position that *any* sharing of data suffices to establish standing. But *Eichenberger* demonstrates the opposite. The Ninth Circuit was not addressing a free-standing, amorphous invasion of privacy injury, but rather a specific Congressional statute defining a particular, categorical injury (unconsented-to disclosure of video-viewing history) to a particular group of people (consumers). *Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 983 & n.1 (9th Cir. 2017); 18 U.S.C. § 2710(b)(1) (a "video tape service provider who knowingly discloses . . . personally identifiable information *concerning any consumer* of such provider shall be liable *to the aggrieved person*" (emphasis added)). In that context, the Ninth Circuit held no additional harm was necessary. As *Spokeo* makes clear, invocation of a statutorily defined injury requires a different Article III standing analysis than would apply to an injury actionable under a different source of law. *Spokeo*, 136 S. Ct. at 1549 ("[I]n the context of a statutory violation," when the injury in fact is an "intangible harm," courts must look to "history and the judgment of Congress" to inform whether the harm is concrete enough for standing purposes); *Eichenberger*, 876 F.3d at 983 (analyzing a VPPA claim under *Spokeo* and concluding the statute protects the "substantive" right to keep "video-viewing history" private).[3] And, as

[2] Contrary to Plaintiffs' parenthetical, *Dugas* did not "find[] standing based on theft of name and credit card information," Opp. 6 n.8. The only injury that was cognizable in *Dugas* was "time and money spent to avoid losses caused by the data breach," *Dugas*, 2016 WL 6523428, at *6, something not at issue in this case.

[3] Even if this Court determines that Plaintiffs have standing under *Eichenberger* (and they do not),

Eichenberger noted, even the VPPA supports Article III standing only for "*unauthorized* disclosure[s]," 876 F.3d at 983 n.1 (emphasis added)—not any disclosure of any information, whether consented-to or not, as Plaintiffs' broad theory would hold. *See* Opp. 6-7.

The VPPA thus expresses Congress's judgment that certain types of plaintiffs—"consumers," as defined by the statute, 18 U.S.C. § 2710(b)(2); *id.* § 2710(a)(1)—have an actionable privacy interest in a certain type of information—"personally identifiable information and video-viewing history," 876 F.3d at 983 (quotation marks omitted); *see* 18 U.S.C. § 2710(a)(3)—and can sue for certain types of wrongful actions that invade such an interest—"unauthorized disclosure[s]" of such information, 876 F.3d at 983 n.1; *see* 18 U.S.C. § 2710(b)(2)(B) (permitting disclosures with consent)—without proof of additional harm. As *Eichenberger* recognized, the VPPA is a "context-specific extension" of historical privacy rights to a new type of information for the purpose of protecting "consumers." 876 F.3d at 983. And Congress's judgment is "instructive" in determining whether the alleged statutory violation is sufficiently "concrete" to satisfy Article III. *Spokeo*, 136 S. Ct. at 1549.

The VPPA is not alone in this regard. The Fair Credit Reporting Act similarly provides that a person who commits a knowing violation of the Act "with respect to any consumer is liable to that consumer." 15 U.S.C. § 1681n(a). The Real Estate Settlement Procedures Act, 12 U.S.C. § 2601 *et seq.*, likewise provides for liability to a particular group of people: "the person or persons charged for the settlement service involved," 12 U.S.C. § 2607(d)(2)—language that indicates Congress's judgment that a particular class of persons suffer an Article III injury for particular types of harm.

The SCA, on the other hand, is a very different statute. Unlike the VPPA, the SCA is not a rights-granting statute; it is a *prohibition* that forbids service providers from "divulg[ing] to any person or entity the contents of a communication." 18 U.S.C. § 2702(a)(1). The SCA does not identify any particular group of people whose rights the statute is protecting or provide for liability to any particular group of people if the law is violated. Thus, only individuals who already have Article III standing are "person[s] aggrieved" under the SCA. *Id.* § 2707(a). Plaintiffs' attempt to transform *Eichenberger* into an across-the-board ruling that "invasion of privacy" can be uttered like an incantation to get through

---

such a finding would apply only to Plaintiffs' VPPA claim. *See* Opp. 5 (conceding that "standing is a claim-by-claim inquiry"). And that claim fails for many other reasons discussed below.

the courthouse doors, Opp. 5, cannot be squared with the case's holding, the statutory language, or the actual claims at issue.

2. Plaintiffs allege no cognizable economic injury

Plaintiffs' claimed economic injuries provide no basis for Article III standing, as this Court has recognized. Pretrial Order No. 16, Dkt. No. 243 ¶ 1 (Jan. 31, 2019); Feb. 1, 2019 Hr'g Tr. 156:3-5. Plaintiffs allude to an undefined "market for personal information." Opp. 8. But even assuming *arguendo* that such a market exists, that says nothing about how Plaintiffs were harmed, nor do Plaintiffs suggest that they could participate in that market. As *Fraley v. Facebook, Inc.*, 830 F. Supp. 2d 785 (N.D. Cal. 2011) recognized, courts have repeatedly dismissed for lack of standing claims in which plaintiffs failed to "articulate how *they* were economically injured by the use of their own information to advertise to themselves" or "how the collection of demographic information was an economic loss to them." *Id.* at 798-99 (collecting cases) (emphasis added). Plaintiffs' attempt to estimate the value of their data *to Facebook* also fails, Opp. 8-9, as it seeks improperly to substitute "a defendant's gain" for the injury in fact requirement, which "must be based on a plaintiff's loss." *Silha v. ACT, Inc.*, 807 F.3d 169, 174–75 (7th Cir. 2015); *see also In re Google, Inc. Privacy Policy Litig.*, 2013 WL 6248499, at *5 (N.D. Cal. Dec. 3, 2013).

Plaintiffs theorize that Facebook appropriated their "first seller advantage," but that too is insufficient to state a constitutionally recognized harm. Opp. 8. The Complaint never alleges that any of the Plaintiffs wanted or tried to be first sellers of their own information. At best, this argument "relies on the 'abstract concept of opportunity costs,'" which is insufficient to support standing. *Goodman v. HTC Am., Inc.*, 2012 WL 2412070, at *7 (W.D. Wash. June 26, 2012).

3. Plaintiffs allege no cognizable risk of identity theft

Plaintiffs have not alleged a credible risk of identity theft because none of the data allegedly provided to third parties is capable of allowing the theft of Plaintiffs' identities, such as social security numbers and financial account information. *See Dugas*, 2016 WL 6523428, at *5 (no standing where theft did not involve "social security information or . . . usernames, passwords, or emails"). Plaintiffs' alleged harms—"increased phone solicitations" or information that is "often used as 'challenge questions'" (without alleging Plaintiffs used them as challenge questions), Opp. 10—are at least one step

removed from any risk of actual identity theft. The potential answers to a challenge question, for example, do a thief no good without the information needed to prompt the challenge question in the first place—such as a Social Security number or credit card number. *See In re Zappos.com, Inc.*, 888 F.3d 1020, 1026 (9th Cir. 2018) (finding standing where an identity thief had "all the information he needed to open accounts or spend money in the plaintiffs' names"). The Court "would have to engage in a hypothetical line of reasoning in order to conclude that" Plaintiffs are "at risk of imminent identity theft given the small amount of useful personal information that a third-party potentially has at its fingertips." *Dugas*, 2016 WL 6523428, at *5; *see also Antman v. Uber Techs., Inc.*, 2015 WL 6123054, at *11 (N.D. Cal. Oct. 19, 2015) (concluding that theft of plaintiff's name and driver's license was insufficient to demonstrate injury in fact because any harm that would result from such a misappropriation posed no credible risk of identity theft).

As for Plaintiffs' alleged investment in "some type of monitoring service," Opp. 10, the Supreme Court has already made clear that Plaintiffs cannot create standing for themselves by "incurr[ing] certain costs," even "as a reasonable reaction to a risk of harm," *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 416 (2013).

B. Plaintiffs Consented to the Challenged Practices, Expressly and By Implication

1. Plaintiffs gave their express consent

As discussed above, Plaintiffs' consent eliminates their standing to sue. It also defeats their claims on the merits. Facebook's Data Use Policy and SRR explained to users exactly how it would share data with third parties, how users could modify or restrict that sharing, and how Facebook would use information to show users targeted advertising. These documents reflect binding contracts between Plaintiffs and Facebook, and Plaintiffs' claims fail because they gave their express consent to each of the complained-of practices. *Smith v. Facebook, Inc.*, 745 F. App'x 8, 8-9 (9th Cir. 2018). In response, Plaintiffs recycle the same erroneous contentions from the last round of briefing: that the Data Use Policy was not part of the SRR, even though the SRR referred to it in several places, and that users did not agree to the Data Use Policy at sign-up, even though users were clearly prompted to review the Data Use Policy before creating their Facebook accounts. Opp. 17. Both contentions are incorrect. *See* MTD 24-26.

Plaintiffs also assert that users were bound only by the version of the SRR and Data Use Policy

in effect when they created their accounts, but that is wrong as a matter of law. Plaintiffs previously conceded that Facebook (i) told users it would post changes to its SRR on the Facebook Site Governance Page, (ii) told users how they could receive notice of future changes, (iii) in fact posted such changes on the Facebook Site Governance Page, and that (iv) Plaintiffs have continued to use Facebook to the present day. Prior Compl. ¶¶ 237, 291, 21-87. Courts frequently enforce updated terms where users continue using a service after the provider gives notice of updated terms. *See In re Facebook Biometric Info. Privacy Litig.*, 185 F. Supp. 3d 1155, 1167 (N.D. Cal. 2016); *Facebook Inc. v. Profile Tech., Ltd.*, 2013 WL 3815886, at *3 (N.D. Cal. July 22, 2013); *Matera v. Google, Inc.*, 2016 WL 5339806, at *17 (N.D. Cal. Sept. 23, 2016); *DeVries v. Experian Info. Sols., Inc.*, 2017 WL 733096, at *7–8 (N.D. Cal. Feb. 24, 2017). The internet could not function any other way.

2. Plaintiffs impliedly consented

Even if Plaintiffs did not expressly consent, Plaintiffs gave their implied consent to share data with third parties. Through the clear disclosures in its binding contracts, *see supra*, the layered disclosures throughout its website, and the widely publicized 2011 FTC Complaint and 2012 Consent Order, users were "on inquiry notice of the terms" of Facebook's services. *Nguyen v. Barnes & Noble Inc.*, 763 F.3d 1171, 1177 (9th Cir. 2014).

First, the terms of the SRR and the Data Use Policy informed users of every challenged practice. *See supra.* Facebook made these polices readily available to users—both at the moment they signed up for Facebook and throughout the user experience by posting a link at the bottom of every page. MTD 27. Plaintiffs again complain about the number of clicks it would take to read the entire Data Use Policy, Opp. 20, but they do not dispute that the Data Use Policy directed users to relevant portions of the policy via prominent subheadings, such as "**Sharing with other websites and applications**" and "**Controlling what is shared when the people you share with use applications.**" MTD 27 (quotation marks omitted).

The Data Use Policy was sufficiently prominent at sign-up to put users on notice of its terms, Opp. 20; *see Nevarez v. Forty Niners Football Co.*, 2017 WL 3492110, at *11 (N.D. Cal. Aug. 15, 2017) (express consent to website's terms where defendant provided plaintiffs with hyperlink to the terms when registering for the account), and users are charged with knowledge of these policies, even if they choose not to view them. *Fteja v. Facebook, Inc.*, 841 F. Supp. 2d 829, 839–40 (S.D.N.Y. 2012) ("clicking the

hyperlinked phrase is the twenty-first century equivalent of turning over the cruise ticket" to review the terms of service). Users were also on notice of any new terms, which were posted on Facebook's Site Governance Page. Prior Compl. ¶¶ 237, 291; *In re Facebook Biometric Info. Privacy Litig.*, 185 F. Supp. 3d at 1167; *Profile Tech*, 2013 WL 3815886, at *3; *Matera*, 2016 WL 5339806, at *17; *DeVries*, 2017 WL 733096, at *7–8.

Second, the app settings contained detailed controls that allowed users to decide which information to share with apps, or to eliminate all such sharing entirely. Plaintiffs suggest that these disclosures were insufficient to tell users that their "Privacy Settings" did not limit sharing with apps. Opp. 19. But the Privacy Settings screen on its face restricts only the people *on Facebook* who can view user data—"Everyone," "Friends of Friends," "Friends," or some "Custom" list. Compl. ¶ 346. Of course, those settings, in turn, affect who has access to a user's data and therefore who has the ability to share the user's data with apps, just as the Data Use Policy explained. D.D., Ex. 45 at 9 ("[I]f you share something on Facebook, anyone who can see it can share it with others, including the games, applications, and websites they use.") And the app settings page made clear that individuals who can see user information on Facebook can "bring it with them when they use Apps," and that the only way to limit all sharing is to "turn off all [P]latform apps." *See* MTD 27-28 (quotation marks omitted). In addition, the FTC's Complaint and Consent Order put users on notice that users' friends could re-share their data with third-party apps. Plaintiffs' only argument to the contrary is based on an obvious misreading of the Consent Order. *See supra.*

C. Plaintiffs Video Privacy Protection Act ("VPPA") Claim Fails

1. Facebook Is Not A Video Tape Service Provider

The VPPA applies only to companies "engaged in the business … of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials." 18 U.S.C. § 2710(a)(4). Facebook is not such a company. Of course, video is one type of media among many that Facebook allows users to share, but its business is not "significantly tailored" to that purpose. *In re Vizio, Inc., Consumer Privacy Litig.*, 238 F. Supp. 3d 1204, 1221 (C.D. Cal. 2017). Plaintiffs point to the fact that Facebook allows users to "upload, share, like, and comment on videos," and allows third parties to access information regarding "video-related content and information through API feeds." Opp. 26. But the same can be

said about all other data on Facebook, including photographs, news stories, and text entries. If Plaintiffs' allegations were sufficient to turn a company into a Videotape Service Provider, then any website that ever posted a video would be covered by the statute. The word "delivery" in the VPPA should instead be read to cover activities akin to "rental or sale." *McDonnell v. United States*, 136 S. Ct. 2355, 2368 (2016) ("[A] word is known by the company it keeps." (quotation marks omitted)). That does not "'read[] the word "delivery" out of the statute,'" Opp. 26, but rather keeps the statute properly focused on video-centric commercial transactions. *See In re Vizio*, 238 F. Supp. 3d at 1221-22.

2. Facebook Did Not Disclose Personally Identifiable Information

The VPPA provides a remedy only if "personally identifiable information" is disclosed. 18 U.S.C. § 2710(a)(3) (quotation marks omitted). The Ninth Circuit has explained that Personally Identifiable Information ("PII") includes "only that information that would readily permit an ordinary person to identify a specific individual's video-*watching* behavior." *Eichenberger*, 876 F.3d at 985 (emphasis added); *see also In re Hulu Privacy Litig.*, 2014 WL 1724344, at *8 (N.D. Cal. Apr. 8, 2014) ("the statute protects personally identifiable information that identifies … particular videos *that the person watched*." (emphasis added) (quotation marks omitted)); *In re Nickelodeon Consumer Privacy Litig.*, 827 F.3d 262, 290 (3d Cir. 2016) (paradigmatic violation is "a video clerk leaking an individual customer's video rental history"). None of the information Plaintiffs identify would reveal which videos they watched:

- "read_mailbox," which included "Videos uploaded by the user," Opp. 27, show that users provided videos to Facebook, not that they watched videos.
- "read_stream," which includes information regarding videos users may have received via Facebook Messenger, Opp. 27, does not reveal the videos users watched, but simply reflects that another user sent a message that the recipient may or may not have read.
- "Likes," Opp. 27, show only that Plaintiffs clicked a button to "like" a particular page, not that the user actually watched a video. *See* Compl. ¶ 410 ("user_likes" and "friends_likes" "provides access to the list of all the pages the user has liked"). Plaintiffs assert that Facebook also shared users' likes of individual videos, but they do not identify a specific data source that would have provided such information and, in any event, "liking" a video does not mean that you watched it or even obtained it.

- "Tags," Opp. 27, show that someone tagged the user in a video, not that the user watched the video.[4]

D. Plaintiffs' Stored Communications Act ("SCA") Claim Fails

Plaintiffs' claim under the SCA, 18 U.S.C. § 2702(a), fails for several reasons. Importantly, Plaintiffs appear to have abandoned their contention that Facebook is liable under the SCA for "indirectly" disclosing data "to unauthorized parties including Cambridge Analytica and data brokers." *See* MTD 34 (quotation marks omitted); Compl. ¶ 851. Plaintiffs now explain that their SCA claims concern only instances in which "Facebook directly disclosed" information to third parties, Opp. 31, and not for any subsequent disclosure by those third parties to others—such as Kogan's disclosures to Cambridge Analytica. For that reason alone, there can be no SCA violation arising out of the Cambridge Analytica events.

With respect to the direct disclosure of information, there can be no SCA violation where the disclosure is consensual. 18 U.S.C. § 2702(b)(3). Here, Facebook obtained the requisite consent in at least two ways. Facebook users consented—expressly and impliedly—to share their *own* information (and to allow their Facebook friends to share their information) with third parties, including apps and device manufactures, because this practice was disclosed in binding agreements between users and Facebook. *See supra*.[5] In addition, the *users' friends* consented to sharing the users' data with third-party apps, as Plaintiffs concede: Kogan's app, for example, "requested permission from its users, including people who took the [personality] test, to access this information about their Facebook friends." Compl. ¶ 458 (quoting UK ICO report). That is sufficient because the SCA permits a disclosure if it is authorized by the "addressee or intended recipient" of the communication. 18 U.S.C. § 2702(b)(3). Plaintiffs do

[4] Contrary to Plaintiffs' assertion, Opp. 27 n.33, Facebook does not agree that the "friends_actions_video, friends_photo_video_tags, and friends_status" categories disclosed Personally Identifiable Information. Plaintiffs have not explained what information they believe these categories of data would provide to third parties, let alone how such information would constitute PII under the VPPA.

[5] Plaintiffs do not dispute that express consent is sufficient. They contend that "constructive" or "implied in law" consent is not sufficient, Opp. 29, but cite no federal cases for that proposition. Indeed, federal case law shows that implied consent can be sufficient under the SCA. *See Perkins v. LinkedIn Corp.*, 53 F. Supp. 3d 1190, 1212 (N.D. Cal. 2014); *In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 1028 (N.D. Cal. 2014).

not dispute that authorization by the friend, alone, is sufficient under the SCA.[6]

Second, Plaintiffs are not entitled to statutory damages because they have not suffered any actual injury, as required by 18 U.S.C. § 2707(c). *See* MTD 34-35; *supra* pp. 8-10. Plaintiffs argue that the statute permits damages of "any profits made by the violator as a result of the violation." Opp. 30 (quotation marks omitted). But such damages are not available without injury to the Plaintiffs and, in any event, Plaintiffs do not (and cannot) make any showing that Facebook profited from sharing their information with Kogan: Facebook does not sell user data and does not charge apps for the right to access data. Cambridge Analytica paid *Kogan* for the data, not Facebook. Compl. ¶ 455.

E. Plaintiffs' California-Law Claims Fail For The Reasons Previously Stated

Facebook's arguments supporting dismissal of Plaintiffs' California-law claims are set forth in its motion to dismiss, and need not be rehashed here. Suffice it to say that Plaintiffs' opposition brief adds nothing new, though a few important concessions are worth highlighting.

California Constitution. Plaintiffs concede that they must demonstrate a "legally protected privacy interest" in the information that was disclosed. Opp. 32 & n.41 (citing *Hughey v. Drummond*, 2015 WL 4395013, at *11-12 (E.D. Cal. July 16, 2015)). Yet they cite no case supporting their argument that they had such a historically grounded privacy interest in the data at issue here. In *Hughey*, the court found a "legally protected privacy interest" in electronic equipment that "contained client-attorney communications and files"—materials protected by an ancient common-law privilege. 2015 WL 4395013, at *11-12. And *Facebook v. Superior Court*, 15 Cal. App. 5th 729, 738 (2017), involved no privacy claim at all.

Common-law claim for public disclosure of private facts. Plaintiffs concede that such a claim arises only where there has been "mass exposure" of private information. Opp. 34 (citing *Kinsey v. Macur*, 107 Cal. App. 3d 265, 272 (1980)). No such exposure is alleged in this case; to the contrary, Plaintiffs identify only a single entity (Cambridge Analytica) that allegedly may have obtained their

[6] Plaintiffs assert that "[w]here communications are configured to be accessible only to specific recipients, they cannot be disclosed without clear consent." Opp. 30 & n.36. But that statement says nothing about *who* can consent. The cases Plaintiffs cite—*Facebook v. Superior Court*, 4 Cal. 5th 1245 (2018), and *In re Facebook, Inc.*, 923 F. Supp. 2d 1204 (N.D. Cal. 2012)—concerned efforts to subpoena communications *without* consent from *either* the senders *or* the recipients.

data. Plaintiffs argue that *Del Llano v. Vivint Solar, Inc.*, 2018 WL 656094 (S.D. Cal. Feb. 1, 2018), did not involve "disclosure or release of private information at all," Opp. 34 n.45, but in fact the case examined whether a plaintiff had "standing [to bring] his invasion of privacy claim," which turned on "publicity in the sense of communication to the public in general or to a large number of persons," 2018 WL 656094, at *5 (quotation marks omitted).

Negligence claim. Plaintiffs concede that they "do *not* ground [Facebook's duty of care] in the contracts between Facebook and Plaintiffs," but rely instead on the existence of a "special relationship." Opp. 39 (citing *J'Aire Corp. v. Gregory*, 24 Cal. 3d 799, 804 (1979)). But, as set forth in Facebook's motion to dismiss, MTD 43-44, the *J'Aire* factors demonstrate that no such special relationship exists.

UCL claim. Plaintiffs concede they are limited to seeking "restitution." Opp. 37. They argue for the return of their "personal content and information," contending that Facebook allegedly "took more content than [it was] entitled to." *Id*. But California law is clear that "'personal information' does not constitute money or property under the UCL." *In re iPhone Application Litig.*, 2011 WL 4403963, at *14 (N.D. Cal. Sept. 20, 2011); *see also Ruiz v. Gap, Inc.*, 540 F. Supp. 2d 1121, 1127 (N.D. Cal. 2008) (finding no "authority to support the contention that unauthorized release of personal information constitutes a loss of property").

In short, Plaintiffs' state-law claims fail at every turn, either because Plaintiffs consented to the sharing of their data, because Plaintiffs had no legally cognizable privacy interest in the data under common law, because Plaintiffs suffered no qualifying injury from the sharing of their data, or because the conduct at issue was governed by contracts between Facebook and Plaintiffs that Facebook is not alleged to have breached—or because of a combination of some or all of the above reasons.

F. Plaintiffs' Claims Are Barred By The Statute of Limitations

Plaintiffs' claims also fail because the 2011 FTC Complaint provided Plaintiffs with constructive notice of their claims. Plaintiffs argue for tolling of the statute of limitations, asserting that Facebook engaged in "bad practices" that amount to "fraudulent concealment." Opp. 43-44 (citing *ShopKo Stores Operating Co. v. Balboa Capital Corp.*, 2017 WL 3579879, at *5 (C.D. Cal. July 13, 2017)). But Plaintiffs do not allege fraudulent concealment in their Complaint. And, in any event, Plaintiffs' argument

ignores the proper inquiry, which focuses on when *Plaintiffs* had reason "to at least suspect that a type of wrongdoing" has occurred. *Fox v. Ethicon Endo-Surgery, Inc.*, 35 Cal. 4th 797, 806-07 (2005). By Plaintiffs' own admission, the 2011 FTC Complaint "outline[d] many of the same issues" as Plaintiffs' Complaint. Compl. ¶ 381. Even if the Plaintiffs took some misguided comfort in the FTC Consent Order (believing it prohibited friend re-sharing of data, which it plainly did not), Opp. 43 (emphasis omitted), "allay[ing]" concerns does not eliminate them. Plaintiffs were on notice of the challenged practices early this decade, and must account for their choice to wait before bringing this lawsuit.

Plaintiffs also argue that the 2015 *Guardian* article did not start the limitations period because it "did not put users on notice about the conduct at issue in this lawsuit." Opp. 44. But the article provided all the key information underlying Plaintiffs' allegations. It stated, for example, that Cambridge Analytica improperly obtained the data of "tens of millions of Facebook users, harvested largely without their permission," including "names, locations, birthdays, genders—as well as . . . Facebook 'likes.'" H. Davies, *Ted Cruz using firm that harvested data on millions of unwitting Facebook users*, The Guardian (Dec. 11, 2015), https://bit.ly/2lHR0Ac. Even the article's title—"Ted Cruz using firm that harvested data on millions of unwitting Facebook users"—should have alerted Plaintiffs that Cambridge Analytica may have accessed their data.

G. The Court Should Dismiss With Prejudice

At the last hearing, the Court instructed Plaintiffs that "the amended complaint will, absent extraordinary circumstance, reflect the plaintiffs' best and final shot at alleging standing and stating a claim." Dkt. 247. Plaintiffs seek leave to amend, but do not identify any extraordinary circumstance that would warrant yet another bite at the apple. Opp. 45. Facebook has raised all of these dismissal grounds before, so none comes as a surprise. *Contra Desertrain v. City of Los Angeles*, 754 F.3d 1147, 1154 (9th Cir. 2014) (cited in Opp. 45). Plaintiffs instead speculate that additional evidence may become public that might "save" their otherwise deficient claims, citing two news articles published after the filing of the amended complaint. Opp. 3 n.7, 21 n.19, 45 & n.56. But they do not explain how those news articles or any future news reports might cure their deficient allegations. Indeed, by Plaintiffs' theory, no deficient complaint could ever be dismissed, as there might always be a hope that more information might emerge. It is time for this litigation to end.

IV. CONCLUSION

For the foregoing reasons, Facebook respectfully requests that this Court dismiss Plaintiffs' Consolidated Complaint without leave to amend.

DATE: May 3, 2019

Respectfully submitted,

GIBSON, DUNN & CRUTCHER, LLP

By: */s/ Orin Snyder*

Orin Snyder (*pro hac vice*)
osnyder@gibsondunn.com
GIBSON, DUNN & CRUTCHER LLP
200 Park Avenue
New York, NY 10166-0193
Telephone: 212.351.4000
Facsimile: 212.351.4035

Joshua S. Lipshutz (SBN 242557)
jlipshutz@gibsondunn.com
GIBSON, DUNN & CRUTCHER LLP
1050 Connecticut Avenue, N.W.
Washington, DC 20036-5306
Telephone: 202.955.8500
Facsimile: 202.467.0539

Kristin A. Linsley (SBN 154148)
klinsley@gibsondunn.com
Brian M. Lutz (SBN 255976)
blutz@gibsondunn.com
GIBSON, DUNN & CRUTCHER LLP
555 Mission Street, Suite 3000
San Francisco, CA 94105-0921
Telephone: 415.393.8200
Facsimile: 415.393.8306

Attorneys for Defendant Facebook, Inc.